Protecting Critical Infrastructures and Key Assets

Terrorists are opportunistic. They exploit vulnerabilities we leave exposed, choosing the time, place, and method of attack according to the weaknesses they observe or perceive. Increasing the security of a particular type of target, such as aircraft or buildings, makes it more likely that terrorists will seek a different target. Increasing the countermeasures to a particular terrorist tactic, such as hijacking, makes it more likely that terrorists will favor a different tactic.

Protecting America's critical infrastructure and key assets is thus a formidable challenge. Our open and technologically complex society presents an almost infinite array of potential targets, and our critical infrastructure changes as rapidly as the marketplace. It is impossible to protect completely all targets, all the time. On the other hand, we can help deter or deflect attacks, or mitigate their effects, by making strategic improvements in protection and security. Thus, while we cannot assume we will prevent all terrorist attacks, we can substantially reduce America's vulnerability, particularly to the most damaging attacks.

All elements of our society have a crucial stake in reducing our vulnerability to terrorism; and all have highly valuable roles to play. Protecting America's critical infrastructure and key assets requires an unprecedented level of cooperation throughout all levels of government-with private industry and institutions, and with the American people. The federal government has the crucial task of fostering a collaborative environment, and enabling all of these entities to work together to provide America the security it requires.

What must we protect? The USA PATRIOT Act defines critical infrastructure as those "systems and assets, whether physical or virtual, so vital to the

United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters." Our critical infrastructures are particularly important because of the functions or services they provide to our country. Our critical infrastructures are also particularly important because they are complex systems: the effects of a terrorist attack can spread far beyond the direct target, and reverberate long after the immediate damage.

America's critical infrastructure encompasses a large number of sectors. Our agriculture, food, and water sectors, along with the public health and emergency services sectors, provide the essential goods and services Americans need to survive. Our institutions of government guarantee our national security and freedom, and administer key public functions. Our defense industrial base provides essential capabilities to help safeguard our population from external threats. Our information and telecommunications sector enables economic productivity and growth, and is particularly important because it connects and helps control many other infrastructure sectors. Our energy, transportation, banking and finance, chemical industry, and postal and shipping sectors help sustain our economy and touch the lives of Americans everyday.

Critical Infrastructure Sectors

Agriculture
Food
Water
Public Health
Emergency Services
Government
Defense Industrial Base
Information and Telecommunications
Energy
Transportation
Banking and Finance
Chemical Industry
Postal and Shipping

The assests, functions, and systems within each critical infrastructure sector are not equally important. The transportation sector is vital, but not every bridge is critical to the Nation as a whole. Accordingly, the federal government will apply a consistent methodology to focus its effort on the highest priorities, and the federal budget will differentiate resources required for critical infrastructure protection from resources required for other important protection activities. The federal government will work closely with state and local governments to develop and apply compatible approaches to ensure protection for critical assests, systems, and functions at all levels of society. For example, local schools, courthouses, and bridges are critical to the communities they serve.

Protecting America's critical infrastructure and key assests requires more than just resources. The federal government can use a broad range of measures to help enable state, local, and private sector entities to better protect the assests and infrastructures they control. For example, the government can create venues to share information on infrastructure vulnerabilities and best-practice solutions, or create a more effective means of providing specific and useful threat information to non-federal entities in a timely fashion.

In addition to our critical infrastructure, our country must also protect a number of key assets—individual targets whose destruction would not endanger vital systems, but could create local disaster or profoundly damage our Nation's morale or confidence. Key assets include symbols or historical attractions, such as prominent national, state, or local monuments and icons. In some cases, these include quasi-public symbol that are identified strongly with the United States as a Nation, and fall completely under the jurisdiction of state and local officials or even private foundations. Key assets also include individual or localized facilities that deserve special protection because of their destructive potential or their value to the local community.

Finally, certain high-profile events are strongly coupled to our national symbols or national morale and deserve special protective efforts by the federal government.

National Vision

The United States will forge an unprecedented level of cooperation throughout all levels of government, with private industry and institutions, and with the American people to protect our critical infrastructure and key assets from terrorist attack. Our country will continue to take immediate and decisive action to protect assets and systems that could be attacked with catastrophic consequences. We will establish a single office within the Department of Homeland Security to work with the federal departments and agencies, state and local governments, and the private sector to implement a comprehensive national plan to protect critical infrastructure and key assets. The national infrastructure protection plan will organize the complementary efforts of government and private institutions to raise security over the long term to levels appropriate to each target's vulnerability and criticality. The federal government will work to create an environment in which state, local, and private entities can best protect the infrastructure they control. The Department of Homeland Security will develop the best modeling and simulation tools to understand how our increasingly complex and connected infrastructures behave, and to shape effective protection and response options. The Department of Homeland Security will develop and coordinate implementation of tiered protective measures that can be tailored to the target and rapidly adjusted to the threat. The Department of Homeland Security, working through the Department of State, will foster international cooperation to protect shared and interconnected infrastructure.

Major Initiatives

Unify America's infrastructure protection effort in the Department of Homeland Security. Our country requires a single accountable official to ensure we address vulnerabilities that involve more than one infrastructure sector or require action by more than one agency. Our country also requires a single accountable official to assess threats and vulnerabilities comprehensively across all infrastructure sectors to ensure we reduce the overall risk to our country, instead of inadvertently shifting risk from one potential set of targets to another. Under the President's proposal, the Department of Homeland Security will assume responsibility for integrating and coordinating federal infrastructure protection responsibilities.

The Department of Homeland Security would consolidate and focus the activities performed by the Critical Infrastructure Assurance Office (currently part of the Department of Commerce) and the National Infrastructure Protection Center (FBI), less those portions that investigate computer crime. The Department would augment those capabilities with the Federal Computer Incident Response Center (General Services Administration), the Computer Security Division of the National Institute of Standards and Technology (Commerce), and the National Communications System (Defense).

The Department of Homeland Security would also unify the responsibility for coordinating cyber and physical infrastructure protection efforts. Currently, the federal government divides responsibility for cyber and physical infrastructure, and key cyber security activities are scattered in multiple departments. While securing cyberspace poses unique challenges and issues, requiring unique tools and solutions, our physical and cyber infrastructures are interconnected. The devices that control our physical systems, including our electrical distribution system, transportation systems, dams, and other important infrastructure, are increasingly connected to the Internet. Thus, the consequences of an attack on our cyber infrastructure can cascade across many sectors. Moreover, the number, virulence, and maliciousness of cyber attacks have increased dramatically in recent years. Accordingly, under the President's proposal, the Department of Homeland Security will place an especially high priority on protecting our cyber infrastructure.

Reducing America's vulnerability to terrorism must also harness the coordinated effort of many federal departments and agencies that have highly specialized expertise and long-standing relationships with industry. For example, the Treasury Department chairs the Financial and Banking Information Infrastructure Committee, which brings together several federal agencies and the private sector to focus on issues related to the financial services industry. Each of the critical infrastructure sectors has unique characteristics, hence posing unique security challenges. The Department of Homeland Security would coordinate the activities of the federal departments and agencies to address the unique security challenges of each infrastructure sector. The following chart depicts the federal government's organization for protecting America's infrastructure and key assests, and indicates the departments and agencies that have primary responsibility for interacting with particular critical infrastructure sectors.

Federal Government Organization to Protect Critical Infrastructure and Key Assets

President

Secretary of Homeland Security

Federal, state, local, and private sector coordination and integration
Comprehensive national infrastructure protection plan
Mapping threats to vulnerabilities and issuing warnings

Sector	Lead Agency
Agriculture	Department of Agriculture
Food:	
Meat and poultry	Department of Agriculture
All other food products	Department of Health & Human Services
Water	Environmental Protection Agency
Public Health	Department of Health & Human Services
Emergency Services	Department of Homeland Security
Government:	
Continuity of government	Department of Homeland Security
Continuity of operations	All departments and agencies
Defense Industrial Base	Department of Defense
Information and Telecommunications	Department of Homeland Security
Energy	Department of Energy
Transportation	Department of Homeland Security*
Banking and Finance	Department of the Treasury
Chemical Industry and Hazardous Materials	Environmental Protection Agency
Postal and Shipping	Department of Homeland Security
National Monuments and Icons	Department of the Interior

* Under the President's proposal, the Transportation Security Administration, responsible for securing our Nation's transportation systems, will become part of the Department of Homeland Security. The new Department will coordinate closely with the Department of Transportation, which will remain responsible for transportation safety.

Build and maintain a complete and accurate assessment of America's critical infrastructure and key assets. The Department of Homeland Security must be able to translate threat information into appropriate action in the shortest possible time, a critical factor in preventing or mitigating attacks, particularly those involving weapons of mass destruction. Accordingly, the Department would build and maintain a complete, current, and accurate assessment of vulnerabilities and preparedness of critical targets across critical infrastructure sectors. The Department would thus have a crucial capability that does not exist in our government today: the ability to continuously evaluate threat information against our current vulnerabilities, inform the President, issue warnings, and effect action accordingly. As noted in the *Intelligence and Warning* chapter, the Department would augment this unique capability with "red team" techniques to view our vulnerabilities from the perspective of terrorists, and to provide objective data on which to base infrastructure protection standards and performance measures.

A complete and thorough assessment of America's vulnerabilities will not only enable decisive near-term action, but guide the rational long-term investment of effort and resources. For example, a comprehensive assessment of vulnerabilities and threats can help determine whether to invest in permanent, physical "hardening" of a target, or in maintaining a reserve of personnel and equipment that can meet a temporary "surge" requirement for increased security.

Enable effective partnership with state and local governments and the private sector. Government at the federal, state, and local level must actively collaborate and partner with the private sector, which controls 85 percent of America's infrastructure. Private firms bear primary and substantial responsibility for addressing the public safety risks posed by their industries-protecting a firm's assets and systems is a matter of sound corporate governance. In many cases private firms, not the government, possess the technical expertise and means to protect the infrastructure they control. Government at all levels must enable, not inhibit, the private sector's ability to carry out its protection responsibilities. The Nation's infrastructure protection effort must harness the capabilities of the private sector to achieve a prudent level of security without hindering productivity, trade, or economic growth.

The Department of Homeland Security would give state and local agencies and the private sector one primary contact instead of many for coordinating protection activities with the federal government, including vulnerability assessments, strategic planning efforts, and exercises. The Department would include an office which reports directly to the Secretary dedicated to this function, and would build on current outreach efforts of existing federal agencies with infrastructure protection responsibilities.

When the Department of Homeland Security learns of a potential threat to our critical infrastructure, it must not only disseminate warnings quickly, but must rapidly map those threats against an accurate assessment of our country's vulnerabilities and effect appropriate action. To ensure this, the government must facilitate and encourage private firms to share important information about the infrastructure they control. Private firms should have reasonable assurance that good faith disclosures about vulnerabilities and preparedness do not expose the firm to liability, drops in share value, loss of competitive advantage, or antitrust action. As discussed in the *Law* chapter, the Attorney General will convene a panel to propose any legal changes necessary to enable sharing of essential homeland security related information between the government and the private sector.

Develop a national infrastructure protection plan. The Department of Homeland Security would develop and coordinate implementation of a comprehensive national plan to protect America's infrastructure from terrorist attack. The plan will build on the baseline physical and cyber infrastructure protection plans which the Office of Homeland Security and the President's Critical Infrastructure Protection Board will release by the end of Fiscal Year 2002. The national plan will provide a methodology for identifying and prioritizing critical assets, systems, and functions, and for sharing protection responsibility with state and local government and the private sector. The plan will establish standards and benchmarks for infrastructure protection, and provide a means to measure performance. The plan will inform the Department of Homeland Security's annual process for planning, programming, and budgeting of critical infrastructure protection activities, including research and development.

As discussed in the *Costs of Homeland Security* chapter, the national infrastructure protection plan will also provide an approach for rationally balancing the costs and benefits of increased security according to the threat—to help answer, in effect, "how much protection is enough?" The plan will describe how to use all available policy instruments to raise the security of America's critical infrastructure and key assets to a prudent level, relying to the maximum possible extent on the market to provide appropriate levels of security. The Department would manage federal grant programs for homeland security, which may be used to assist state and local infrastructure protection efforts. In some

cases, the Department may seek legislation to create incentives for the private sector to adopt security measures or invest in improved safety technologies. In other cases, the federal government will need to rely on regulation—for example, to require commercial airlines to electronically transmit passenger manifests on international flights, or to require permits for intrastate purchase of explosives.

Securing cyberspace. The cost to our economy from attacks on our information systems has grown by 400 percent in four years according to one estimate, but is still limited. In one day, however, that could change. Every day somewhere in America an individual company or a home computer user suffers what for them are significantly damaging or catastrophic losses from cyber attacks. The ingredients are present for that kind of damage to occur on a national level, to our national networks and the systems they run upon, on which the nation depends. Our potential enemies have the intent; the tools of destruction are broadly available; the vulnerabilities of our systems are myriad and well-known. In cyberspace, a single act can inflict damage in multiple locations simultaneously without the attacker ever having physically entered the United States.

Accordingly, the President acted quickly following the terrorist attacks in September to secure our information and telecommunications infrastructure. The President created the Critical Infrastructure Protection Board and launched a public-private partnership to create a *National Strategy to Secure Cyberspace*. The *National Strategy to Secure Cyberspace* will provide a roadmap to empower all Americans to secure the part of cyberspace they control, including a variety of new proposals aimed at five levels: the home user and small business; large enterprises; sectors of the economy; national issues; and global issues.

Thousands of citizens all across the country have contributed to the effort by contributing their views in Town Hall meetings, on interactive web sites, or by participating in one of the dozens of participating groups and associations. State and local governments and state and local law enforcement have also united to prepare their own cyber security strategies.

Harness the best analytic and modeling tools to develop effective protective solutions. As discussed in the *Intelligence and Warning* chapter, responding to threat information requires life-or-death decisions that must often be made in conditions of great uncertainty. High-end modeling and simulation tools can greatly enhance our ability to quickly make those decisions based on the best possible understanding of their consequences. State-of-the-art modeling and simulation provides another important tool for determining what assets, systems, and functions are "critical," a process that involves many factors that interact with one another in complex ways. For example, an attack on a key Internet node might cause few casualties directly, but could trigger cascading effects across many infrastructure sectors, causing widespread disruption to the economy and imperiling public safety. An attack on a major port could inflict damage that affects transportation, energy, and economic infrastructure nationwide. A chemical attack would have little effect on an empty stadium; a catastrophic effect on a stadium filled with tens of thousands of spectators. Protecting America's critical infrastructure thus requires that we determine the highest risks based on the best possible understanding of these factors, and prioritize our effort accordingly. The Department of Homeland Security would develop and harness the best modeling, simulation, and analytic tools to evaluate the full range of relevant factors and the complex manner in which they interact. The Department would take as its foundation the National Infrastructure Simulation and Analysis Center (currently part of the Department of Energy).

Guard America's critical infrastructure and key assets against "inside" threats. The "insider threat" and personnel reliability are increasingly serious concerns for protecting critical infrastructure. In the food processing and distribution industry, disgruntled or former employees have caused nearly all previous incidents of food tampering, providing a glimpse of what terrorists with insider access might accomplish. Personnel with privileged access to critical infrastructure, particularly control systems, may serve as terrorist surrogates by providing information on vulnerabilities, operating characteristics, and protective measures. These "insiders" can also provide access to sensitive areas, such as loading docks, control centers, and airport tarmacs. The U.S. government, working through the Department of Homeland Security will undertake a comprehensive review of critical infrastructure personnel surety programs and propose national standards for screening and background checks. To this end, the Secretary of Homeland Security and the Attorney General will convene a panel with appropriate representatives from federal, state, and local government, in consultation with the private sector, to examine whether employer liability statutes and privacy concerns hinder necessary background checks of personnel with access to critical infrastructure facilities or systems. The Department of Homeland Security would also undertake a comprehensive review of other protection measures necessary to deny terrorist access to critical infrastructure—for example, establishing "security zones" and controlling access around

vulnerable port facilities much as we control access at airports.

Partner with the international community to protect our transnational infrastructure. We share much of our critical infrastructure with our neighbors in Canada and Mexico, and increasingly with countries around the world. Our electricity transmission, natural gas and petroleum pipelines are part of a vast, interconnected system that serves not only the United States, but Canada and Mexico as well. America's seaports often contain dense concentrations of population and critical infrastructure assets and systems while sustaining an ever-increasing volume of trade with ports around the globe. Thus, terrorists need not gain access to our territory to attack our infrastructure. The Administration is establishing joint steering committees with both Canada and Mexico to improve the security of critical physical and cyber infrastructure, and is actively pursuing necessary international cooperation to increase the security of global transportation systems and commerce.